Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 627083, 12 pages
http://dx.doi.org/10.1155/2015/627083

Research Article

Wireless Coexistence and Spectrum Sensing in Industrial Internet of Things: An Experimental Study

Jean M. Winter,[1] Ivan Muller,[1] Gloria Soatti,[2] Stefano Savazzi,[3] Monica Nicoli,[2] Leandro Buss Becker,[4] João C. Netto,[5] and Carlos E. Pereira[1]

[1]*Department of Electrical Engineering, Federal University of Rio Grande do Sul, 90035-190 Porto Alegre, RS, Brazil*
[2]*Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, 20133 Milano, Italy*
[3]*National Research Council of Italy (C.N.R.), Institute of Electronics, Computer and Telecommunication Engineering (IEIIT), 20133 Milano, Italy*
[4]*Department of Automation Systems, Federal University of Santa Catarina, 88040-900 Florianopolis, SC, Brazil*
[5]*Institute of Informatics, Federal University of Rio Grande do Sul, 91501-970 Porto Alegre, RS, Brazil*

Correspondence should be addressed to Ivan Muller; ivan.muller@ufrgs.br

Received 18 May 2015; Accepted 12 October 2015

Academic Editor: Iqbal Gondal

The adoption of dense wireless sensor networks in industrial plants is mandatorily paired with the development of methods and tools for connectivity prediction. These are needed to certify the quality (or reliability) of the network information flow in industrial scenarios which are typically characterized by harsh propagation conditions. Connectivity prediction must account for the possible coexistence of heterogeneous radio-access technologies, as part of the Industrial Internet of Things (IIoT) paradigm, and easily allow postlayout validation steps. The goal of this paper is to provide a practical evaluation of relevant coexistence problems that may occur between industrial networks employing standards such as *Wireless*HART IEC 62591, IEEE 802.15.4, and IEEE 802.11. A number of coexistence scenarios are experimentally tested using different radio platforms. For each case, experimental results are analyzed to assess tolerable interference levels and sensitivity thresholds for different configurations of channel overlapping. Finally, the problem of over-the-air spectrum sensing is investigated in real scenarios with heterogeneous industrial networks to enable a cognitive resource allocation that avoids intolerable interference conditions.

1. Introduction

Automation systems have undergone a progressive cable reduction in the last decades since the traditional 4–20 mA for analog communication to digital communication over bus networks such as Fieldbus, Hart and Profibus protocols [1]. A further step in this direction is the current effort of the industrial organizations to promote the use of wireless technologies in industrial applications. The well-known benefits provided by wireless technologies motivated the introduction of different wireless standards for a huge quantity of applications. These circumstances lead to an usual presence of heterogeneous wireless systems in the same coverage area which, many times, compete for the same frequency band. The coexistence of different wireless communication standards may result in interference with detrimental effects such as data loss, jitter, delay in transmission, and loss of synchronization between devices. These issues can often result in unreliable communication that might cause large losses and process failures. Although many attempts have been made to launch an industrial wireless standard (e.g., within the families of networking standards, as Bluetooth, WiFi, and ZigBee), no one of these could fulfill all the industrial requirements [2]. Some standards are able to handle interferences at higher levels, but the techniques that are usually adopted either try to avoid collisions or suggest hopping for unused channels, making the procedures time consuming and reducing the network throughput. The *Wireless*HART protocol (WH) has been introduced for critical industrial applications, followed by others such as ISA.100 and Wireless Networks for Industrial Automation-Process Automation (WIA-PA), with the aim of replacing cabling in process automation. At the

same time, IEEE 802.11 represents an important and highly disseminated standard which fits applications for wireless local area networks (WLAN) and currently provides wireless connectivity for a huge number of portable devices. The IEEE 802.11 standard has a large interoperability between vendors and it is currently well appointed for non-critical industrial applications (e.g., providing connectivity to mobile operators inside the plant [3]).

This work investigates the problem of wireless coexistence and the related issue of interference sensing, focusing on industrial application scenarios and presenting a set of experimental evaluations for the WH, IEEE 802.15.4, and IEEE 802.11 standards. Key aspects of the WH protocol are first analyzed, highlighting the robustness of this wireless networking standard in interference-limited environments (Section 2). A physical (PHY) layer model is then introduced for the evaluation of the connection probability, looking at the problem of coexistence between IEEE 802.11 (WiFi) and IEEE 802.15.4 based standards operating in unlicensed band (Section 3). Several experimental activities on the wireless coexistence problem are discussed, including the analysis of the critical IEEE 802.11 interference threshold that can be tolerated by IEEE 802.15.4 devices in a controlled environment testbed (Section 4) and an over-the-air testbed setup considering different IEEE 802.15.4 PHY layer configurations (e.g., different values for the spread spectrum factor) [4] (Section 5). The coexistence problem is then analyzed experimentally by looking at the WH standard and related link-layer mechanisms (Section 6). Finally, a method for interference detection based on distributed spectrum sensing is discussed and validated by experimental results (Section 7). The method relies on a network of sensing devices that cooperatively identify the overall interference patterns caused by a preexisting network of devices (e.g., primary users). The proposed procedure can be exploited for resources scheduling, jointly with the practical coexistence rules identified in the first part of the paper, in order to avoid intolerable interference conditions [5].

2. *Wireless*HART Protocol

WH is the first international standard for wireless communication in process automation approved by the International Electrotechnical Commission (IEC) for industrial applications. It provides an IEEE 802.15.4 TDMA-based wireless mesh networking technology [6] operating in the unrestricted 2.4 GHz ISM radio band with stringent timing and security requirements.

The TDMA MAC sublayer is built upon the IEEE 802.15.4 PHY layer for mesh network communications and it is responsible for deterministic collision-free communications between HART compatible devices. In the PHY layer, the WH protocol is based on the IEEE 802.15.4 standard, operating within 15 channels of the 2.4 GHz ISM band. It defines superframes of variable length, fixed timeslot of 10 ms (corresponding to 625 OQPSK symbols), network-wide time synchronization, channel hopping scheme, channel blacklisting, and industry-standard AES-128 block ciphers with related keys. The adoption of the TDMA technology with precise network-wide time synchronization was the key feature distinguishing WH with respect to the IEEE 802.15.4 standard. Recently, this MAC mechanism adopted by WH has been standardized and integrated, as an amendment, also into the IEEE 802.15.4 standard (i.e., into IEEE 802.15.4e) referred to as Time-Slotted Channel Hopping (TSCH).

In a TSCH PAN, the concept of superframe is replaced with the "slot frame" one; each slot frame is made of a series of slots allowing communication between synchronized peer nodes. Due to the fact that nodes are assumed to be synchronized (by means of higher-level protocol services outside IEEE 802.15.4), beacons are not required to initiate communications.

The WH protocol introduces a series of mechanisms that increase the system reliability in scenarios with coexistence of other possible sources of interference. These mechanisms are reviewed below, with special focus on MAC and link layer.

2.1. Multipath Routing. WH supports mesh topologies, based on multipath routing techniques. All field devices are able to serve as routers and each field device handles a list of neighbors that are controlled by the network manager (NM). Nodes close enough to be overheard by other devices are kept in a table list named unlinked neighbors. This table is dynamically updated based on information that nodes periodically send to the NM, such as receive signal strength indicator (RSSI) and last communication time. Based on accumulated data (RSSI, packet loss rate, reliability, etc.), the NM can provide a new link between two devices and consequently expand the mesh network. The more the neighbors are, the higher the spatial diversity and the network reliability are. A well designed mesh topology has typically a reliability greater than 99,73% [7].

2.2. TDMA Framework. One distinct feature of the WH standard is the time-synchronized data link layer. WH defines a strict 10 ms timeslot and utilizes a TDMA structure to provide collision-free communications. Time slots are able to accommodate a single transaction consisting of data/command frame and related acknowledgement (ACK) messages.

Integrated ACK is adopted to improve the protocol reliability (note that transmission of ACK message occurs inside the same time slot of the data frame). The transport layer handles the acknowledged service which allows devices to send packets and confirm their delivery. In case of nonsuccessful delivery, transmission retry is scheduled.

Figure 1 illustrates a WH timeslot with the sent message and its acknowledgment. The acknowledgment message also allows synchronous operations across the network, since ACK brings a time adjustment for keeping the TDMA access control.

2.3. Channel Hopping. The WH superframe is periodical, with the total length of the member slots as the period. Superframe transmission starts at network setup from the Absolute Slot Number (ASN) equal to 0. The ASN provides an absolute reference to the current superframe and it is determined by the access point that is also the original timing reference and source for all the wireless devices.

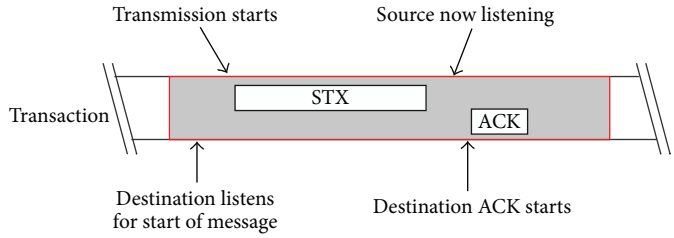


Figure 1: *Wireless*HART: framing structure for acknowledgment.

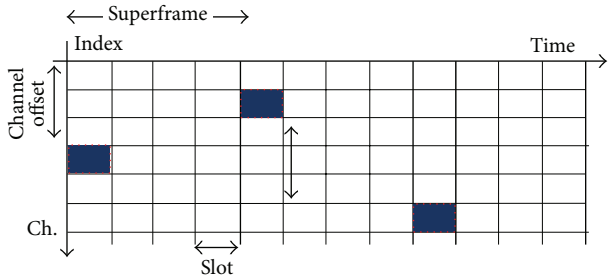


Figure 2: Example of channel hopping mechanism.

Each superframe then repeats itself in the predefined period (e.g., 100 slots corresponding to 1 sec). A logical channel in the WH standard corresponds to a sequence of physical IEEE 802.15.4 channel hopping. Channel hopping defined by WH combines TDMA and frequency hopping to introduce frequency (channel) diversity and time diversity to further reduce the possibility of communication impairment. WH includes a channel hopping scheme (slotted hopping) with variation of patterns by changing different channels. The channel to be used in a designated slot is computed according to

$$\text{Active Channel} = \left(\frac{\text{Channel Offset} + \text{ASN}}{\text{Number of Active Channels}} \right). \quad (1)$$

Based on the availability of multiple channels from the IEEE 802.15.4 PHY layer, the goal of the WH channel hopping scheme is to have each communication link between any two devices hopping over a set of predefined physical channels. The channel set may include all of the available channels or only a subset defined by a blacklist or a whitelist. Blacklisting may be used to avoid conflict with preexisting WH installations. In addition to diversity, channel hopping is also adopted to improve security of communication. Based on (1), in fact, only the devices joining the network know the channels where communication will occur. Figure 2 illustrates a random channel hopping sequence.

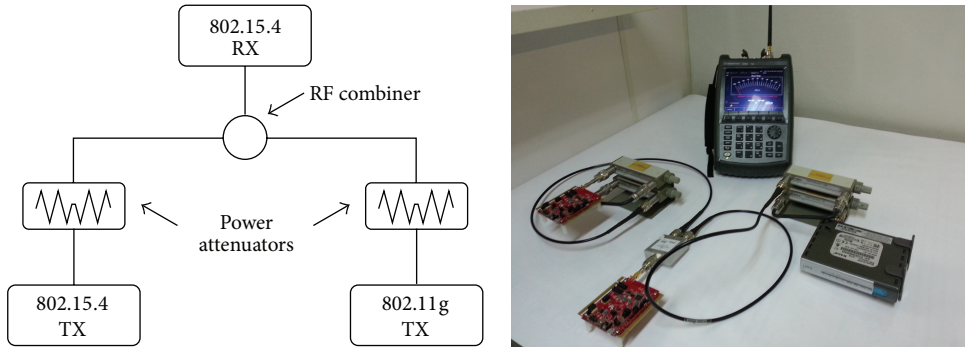
3. Modeling of Coexistence for High Traffic Load

The possibility to exploit multiple and heterogeneous network technologies deployed in close proximity (i.e., for monitoring/controlling [8] the same industrial process) provides an attractive opportunity for efficient resource sharing and traffic off-loading. However, besides offering a large number of benefits, the practical deployment of heterogeneous radio technologies still needs to face some critical issues and design challenges, such as the development of an efficient regulatory framework that preserves Quality of Service (QoS) by interference coordination and network design mechanisms to ensure that the mutual interference is kept below acceptable limits. In this section, we focus on the problem of PHY layer modeling of the coexistence between WiFi and IEEE 802.15.4 based standards operating in the same unlicensed 2400 ÷ 2490 MHz ISM band.

The widely adopted link quality indicator (LQI) or RSSI metric, here denoted as g_l [9] for link l, is not enough to estimate the average probability P_S of successful connection in the presence of interference [4, 10]. In what follows, we focus on the relevant case (in terms of QoS [11]) of IEEE 802.15.4 devices suffering the interference from one WiFi mobile device. The interference power on link l is indicated as μ_l. The traffic load of the interference is modeled as a Bernoulli process, with probability $0 \leq P_\mu \leq 1$ accounting for the degree of frame collisions. The Signal to Interference Ratio, $\text{SIR}_l = g_l/\mu_l$, serves as an additional metric, used jointly with the LQI, for the assessment of the successful connection probability P_S (expressed in terms of frame error rate) as

$$P_S = \begin{cases} P_r\left[g_l > \beta\right], & \text{if } \mu_l < \dfrac{\beta}{\beta_I} \\ P_\mu P_r\left[\text{SIR}_l > \beta_I\right] + \left(1 - P_\mu\right) P_r\left[g_l > \beta\right], & \text{if } \mu_l \geq \dfrac{\beta}{\beta_I}, \end{cases} \quad (2)$$

where the LQI (or RSSI) g_l is modeled as in [10]. The ratio β/β_I indicates the critical value of cochannel disturbance μ_l (captured by the receiver) above which the interference has a relevant impact on the connectivity. The RSSI threshold $\beta = -85$ dBm [9] depends on the receiver sensitivity and limits the performance in interference-free scenarios; the sensitivity β also depends on PHY data-rate settings as described in Section 5. On the other hand, the link margin $\beta_I = \beta_I(\eta)$ depends on the degree of spectrum overlapping $\eta \in [0, 1]$ between the useful signal and the cochannel disturbance, as experimentally verified in Section 4.1. Overlapping is defined as the amount of interference power $\eta \times \mu_l$ lying over the considered IEEE 802.15.4 channel: this is obtained by considering only the portion of the occupied interferer spectrum in common with the useful signal. In what follows, the threshold



(a) (b)

Figure 3: (a) Testbed scenario; (b) experimental equipment.

$\beta_I(\eta)$ is evaluated experimentally for the relevant case (in the industrial context) of IEEE 802.15.4 devices acting as victims of WiFi (IEEE 802.11) interference and subject to full ($\eta \geq 0.5$) or partial ($\eta < 0.5$) spectrum overlapping.

4. WiFi Interference Analysis in Confined Environment

The received signal is the result of a combination of different radio propagation phenomena which depend on the surrounding environment (indoor or outdoor), the number, size and material of scattering objects, noise and interference, and so forth. In the following, a set of experiments is carried out to identify the WiFi interference threshold that is endured by IEEE 802.15.4 devices in a confined environment. This analysis allows reducing the number of variables related to the test environment and eases the identification of the key factors that limit the coexistence (regardless of the specific scenario of deployment).

4.1. Experimental Setup. A testbed is set up to evaluate the IEEE 802.15.4 robustness through a KW20x radio platform [12]. Experiments are conducted using two RF attenuators, a combiner, and IEEE 802.15.4 and IEEE 802.11g compliant radio transceivers. Moreover, a spectrum analyzer is used to measure the power and losses of the devices in different sections of the experiment (output attenuators, combiner, crosstalk, etc.). Figure 3(a) shows the testbed architecture and Figure 3(b) shows the experimental equipment and the physical arrangement.

In the performed experiments, IEEE 802.11 interference has been generated for $\eta \geq 0.5$ and $\eta < 0.5$. The IEEE 802.15.4 PHY channels from 14 to 21 are used under the IEEE 802.11 interference, as illustrated in Figure 4.

The link quality between IEEE 802.15.4 radios is first tested for a fixed output power and without any interference, to guarantee output power levels with a good link quality. In the next step, an IEEE 802.11 interferer is introduced and its power output is increased by 1 dB steps to identify the first packet loss measured by the IEEE 802.15.4 radio devices. By following this procedure, it is possible to identify the critical level of IEEE 802.11 interference power that causes IEEE 802.15.4 packet corruption.

4.2. Analysis and Results. Figure 5 highlights the maximum tolerable SIR (corresponding to minimum values of interference power) that avoids significant performance degradation at the IEEE 802.15.4 radio receiver configured to transmit over channels 14 to 21. This experiment considers a high traffic load scenario [13]: the WiFi network is characterized by a maximum utilization factor while the IEEE 802.15.4 transmitter continuously sends packets of 123 bytes to its peer receiver.

Results demonstrate that for the IEEE 802.15.4 channels 16–19 fully overlapping ($\eta = 1$) with the IEEE 802.11 channel 6, the minimum tolerable SIR has values of 14.1 dB, 15.1 dB, 14.1 dB, and 9.1 dB, respectively. Also, the adjacent channels, 15 and 20, present performance impairments for an interfering signal with a SIR lower than −21.9 dB and −19.9 dB, respectively. Finally, the lowest tolerable SIR is measured over the alternate channels (with $\eta < 0.1$) providing values of −25.9 dB for channel 14 and −23.9 dB for channel 21.

It is important to emphasize that these results may suffer from slight variations depending on the specific radio platform that has been used, especially interference measured in adjacent and alternate channels. The spurious signals that extend the harmonic frequencies may be more or less suppressed for a specific radio transmitter; this variation can also occur between different channels used in the same radio platform. Nevertheless, from the obtained results it is possible to identify a significant order of magnitude for a SIR between IEEE 802.15.4 and IEEE 802.11 without losses.

5. Analysis of Coexistence: Over-the-Air Tests

In this section, we describe the results of over-the-air tests, now with attenuations generated by radio-frequency propagation in mixed line-of-sight (LOS) and non-LOS environments. Critical (or worst-case) high traffic load scenarios are analyzed where a WiFi-Direct peer-to-peer (P2P) network and an IEEE 802.15.4 network are continuously transmitting. Further interference coexistence scenarios are considered and analyzed in [4, 11, 13–15].

The impact of enhanced IEEE 802.15.4 PHY data-rate transmission mode is also discussed. The topic is relevant as enhanced data-rate mode is supported by recent HW designs [13] to comply with delay-sensitive applications. The setup depicted in Figure 6 consists of one IEEE 802.15.4 device that

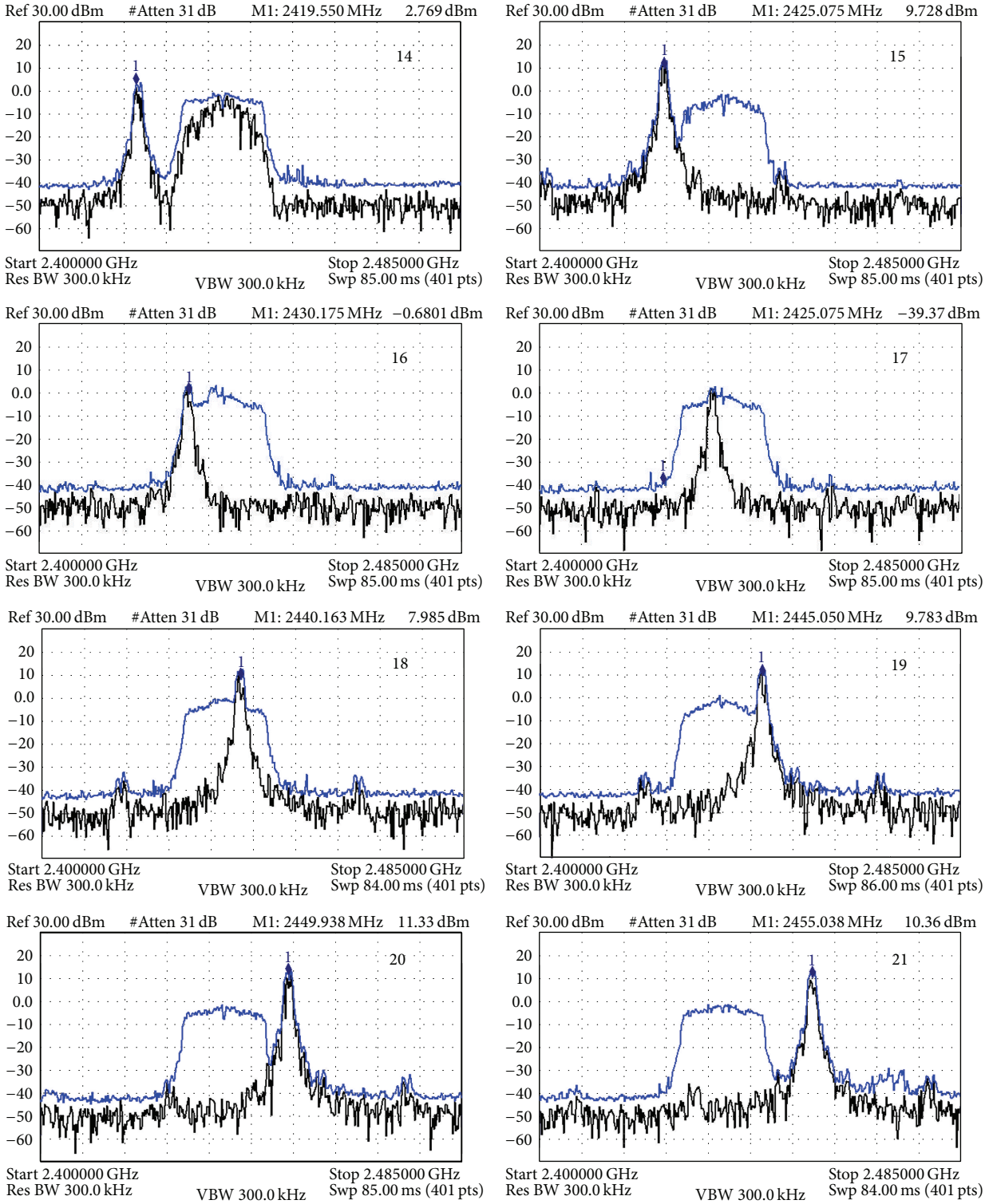


Figure 4: IEEE 802.15.4 channels (black) under IEEE 802.11 interference (blue).

transmits full data frames of 127 bytes towards a Gateway (GW) labeled as node 1. GW nodes can support double radio technology with WiFi Direct and IEEE 802.15.4. The transmitter is a programmable device configured to switch among 7 consecutive channels having bandwidth 5 MHz (with center frequencies ranging from 2405 MHz to 2435 MHz). It sends data in continuous mode by disabling carrier sense multiple access (CSMA) to conform with industry standard PHY [15] and implement a direct-sequence spread spectrum (DSSS) with factor $Q_1 = 8$ and data rate of 250 kbps. The GW

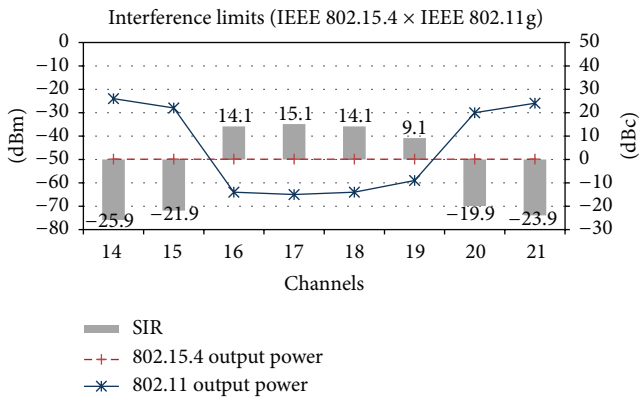


FIGURE 5: Interference threshold (from IEEE 802.11) to corrupt IEEE 802.15.4 packets.

receiver (GW1), located at distances ranging in $d_1 = 4$–10 m, measures the IEEE 802.15.4 link quality in terms of LQI g_l. The GW is also affected by a disturbance (cochannel interference) originated by a WiFi-enabled portable Android device located at varying distances $d_2 = 10$–15 m from GW1 and communicating in P2P mode with GW node (GW2) through WiFi Direct [16] (over IEEE 802.11g) using the band $2400 \div 2420$ MHz. The considered scenarios are characterized by varying interference signal strengths μ_l (accounting for LOS/NLOS propagation and different distances d_2), collision probability P_μ, and spectrum overlapping η, both measured by a 2.4 GHz spectrum analyzer.

In Figure 7 we analyze the successful connection probability P_S evaluated as in (2), for varying SIR, assuming full overlapping $\eta \geq 0.5$ (channels 11–14) and continuous WiFi traffic, with high load as $P_\mu = 1$. Successful probability is obtained by counting the number of successfully acknowledged data frames normalized by the number of frames received with interferer disabled. According to model (2) and results in Section 4, the optimal threshold β_I can be reasonably set to $\beta_I = 15$ dB. As also observed in confined environments, the use of channels experiencing $\eta \geq 0.5$ must be avoided by blacklisting (when possible) for $\mathrm{SIR}_l < 15$ dB. In Figure 7, the probability P_S is also evaluated over 7 consecutive channels to highlight the impact of spectrum overlapping and interference traffic loads. The analysis focuses on the extreme cases of full overlapping with $\eta = 1$ (channels 11–13) and $\eta = 0.5$ (channel 14) and partial overlapping with $\eta < 0.1$ (channels 15–17), being the most meaningful cases observed in the tests. We also consider WiFi-Direct P2P group formation [16] (in dashed lines), with collision probability $P_\mu = 0.1$ and continuous WiFi traffic (in solid lines), with $P_\mu = 1$. The use of partially overlapped channels (15–17) might be reasonably tolerated without significant penalties even at low SIR regime (when $\mathrm{SIR}_l > -6$ dB). Threshold values (in dB scale) for SIR in (2) can be summarized as follows:

$$\beta_I(\eta, Q_1 = 8) \cong \begin{cases} 15\,\mathrm{dB} & \text{for } \eta \geq 0.5 \text{ ch (11–14)} \\ -6\,\mathrm{dB} & \text{for } \eta < 0.5 \text{ ch (15–17)}. \end{cases} \quad (3)$$

5.1. Enhanced IEEE 802.15.4x PHY Data Rate. In this section, we investigate the use of high-data-rate mode as available in recent low-power IEEE 802.15.4 compliant transceiver devices [13]. The use of the enhanced data-rate mode can be a promising option for fast servicing of unexpected conditions that require a fast reaction over the networking, a low-latency mode, and a meaningful increase of the sensor data publishing rate [17]. In Figure 8, the coexistence with WiFi is addressed for the same settings, now by programming the wireless devices to reduce the IEEE 802.15.4 DSSS factor (for payload transmission) down to a value of $Q_2 = 2$, corresponding to a PHY data rate of 1 Mbps. According to our experiments, the IEEE 802.15.4 data frame transmission duration reduces from 4 ms down to 1.6 ms (for a payload of 102 bytes), at the cost of a slightly lower interference-free sensitivity $\beta = -82$ dBm compared to the standard data-rate case. Given that the IEEE 802.15.4 transceiver is continuously transmitting, the observed collision probability P_μ during P2P WiFi group formation is marginally influenced by the reduced transmission duration (and still $P_\mu = 0.1$). Due to the large interference capturing effect, the optimal SIR threshold is larger compared to the standard data-rate case as $\beta_I = \beta_I(\eta, Q_2 = 2) = 21$ dB. Optimal threshold can be therefore reasonably modeled as a linear function of (2):

$$\beta_I(\eta, Q_2 = 2) \cong \beta_I(\eta, Q_1) + \left[\frac{Q_1}{Q_2}\right] \mathrm{dB} \quad (4)$$

as increasing with the ratio of spreading factors $[Q_1/Q_2]\mathrm{dB} = 6$ dB.

6. *Wireless*HART under IEEE 802.15.4 Interference

In this section, we evaluate the performance of WH subject to interference. Average latency and packet error rate are analyzed as key indicators of service quality. Compared to the testbeds presented in Sections 4 and 5 some changes are done: the IEEE 802.11 device is now replaced by a WH field device and the IEEE 802.15.4 RX device is replaced by a WH gateway (WH-GW) acting as network manager. The equipment physical disposal is similar to the setup presented in Figure 5. With these modifications, a new experiment is conducted. In this testing scenario one WH-GW is connected with one field device which simplifies the analysis but still provides comparable results with respect to the experiments in the controlled environment.

The interference signal considered in the experiment now consists of a continuous transmission of IEEE 802.15.4 frames with full payload and high output power, enough to corrupt IEEE 802.15.4 packets as demonstrated in earlier results. The experiments are performed in three stages, each one with a period of 72 hours. In the first stage, no interference is introduced; in the second one, an IEEE 802.15.4 transmitter is interfering with the WH network configured to operate over 15 channels; in the last stage, the available WH channels are reduced to 5 (by blacklisting the remaining channels) with one channel fully overlapped with the IEEE 802.15.4 interference signal. Table 1 summarizes the obtained results.

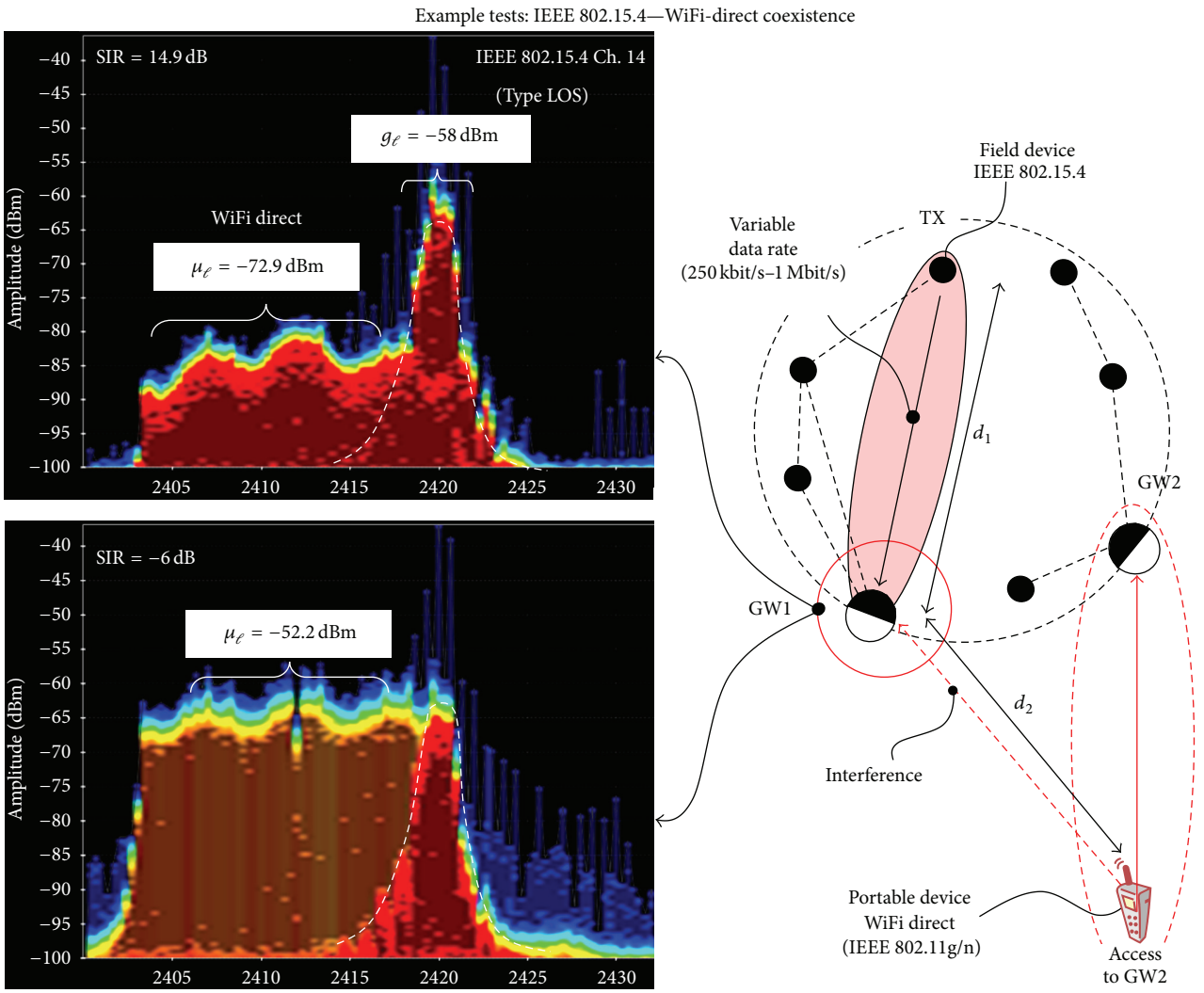


Figure 6: Heterogeneous WiFi-IEEE 802.15.4 network scenario: a portable WiFi-enabled device is communicating with gateway GW2 by WiFi Direct. Interference (with varying power μ_l and SIR, see two examples) is observed at gateway GW1 by the spectrum analyzer. The IEEE 802.15.4 GW1 receiver is thus suffering as victim of WiFi interference.

Table 1: Measures from WH performance under interference conditions.

Stages	TX packets	TX failed	RX packets	Packet error rate	IEEE 802.15.4 interference	WH channels available	Average latency
1	65320	181	1029	0.28%	Off	15	0.720 s
2	75840	9398	960	12.39%	On	15	0.826 s
3	108726	39108	796	35.97%	On	5	1.540 s

Focusing on the first stage (corresponding to the interference free scenario), the results show a negligible packet error rate (about 0.28%) and a network latency of 0.720 seconds. Latency accounts for scheduling time of messages (by the field device), transmission over the wireless medium, and payload decoding at the WH-GW. Observed latency is averaged over consecutive transmissions.

In the second stage of the experiment, all WH channels are available to the WH-GW and the IEEE 802.15.4 interference signal is generated on channel 18, which is centered in 2440 MHz. It is possible to observe an increased amount of failed transmission sessions corresponding to transmitted packets without ACK. Results show a packet error rate of 12% and a latency increase of 14%.

Stage 3 represents a worst case setting where only channels 16, 17, 18, 19, and 20 are available for WH networking, while similarly as for stage 2 the IEEE 802.15.4 interference signal is configured to occupy channel 18. In this case, the observed packet losses are 35% while latency is 1.540 seconds.

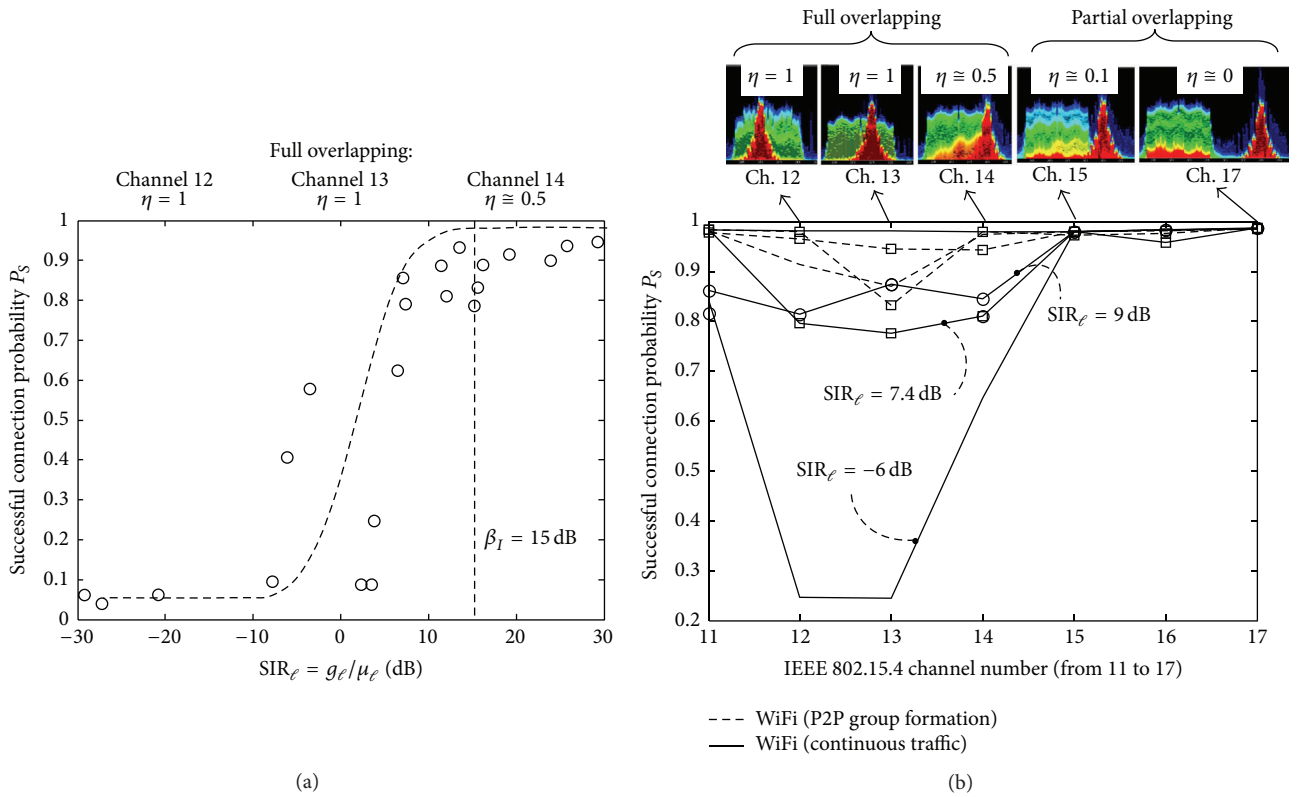


Figure 7: Successful probability (IEEE 802.15.4 packets) for varying SIR under full overlapping (a). Successful probability for varying WiFi-IEEE 802.15.4 overlapping (b), for selected values of SIR and traffic loads, under continuous transmission and P2P WiFi group formation. IEEE 802.15.4 (standard 250 kbps, DSSS $Q_1 = 8$).

In order to get further insight into the results summarized in Table 1, an analysis of the network resource distribution undergone by the network manager is provided next. As introduced in Section 2, *Wireless*HART makes use of superframes, which consist of time slots with cyclic occurrence: slots are preassigned to devices by the network manager. Observed latency in case of transmission failures is ruled by the number of slots assigned for a specific device and the interval between them. Figure 9 highlights the time interval between slots for the field device under testing. The assigned slots for data publication have been identified through a WH network analysis software, previously developed.

For the device under test, the slot numbers 34, 286, 429, 625, and 795 are programmed for data publication inside each superframe (of length 1024 slots), while slots have 10 ms size. The field device is configured to continuously transmit process values every 4 seconds. Thus, during the 4-second transmission session three transmission opportunities are available over three slots configured for different WH channels (and frequencies). In case packet drops occur during transmission in one of those slots, the next transmission opportunity is automatically scheduled to the next slot over a WH channel not suffering from the IEEE 802.15.4 interference. For example, analyzing stage 3, it is possible to observe that the average latency can be approximated as the distance between two consecutive slots (about 1.5 seconds), corresponding to a transmission failure in one channel (corrupted by IEEE 802.15.4 interference) followed by success in the next one (interference-free). Given that 5 channels are available, the probability of collision with IEEE 802.15.4 transmission ($P_\mu = 1/5$) serves as reasonable approximation to the observed packet loss rate. Although it is not considered here as focusing on point-to-point communication, the superframe routing policy also affects the latency results as pointed out in [18, 19].

Although the observed number of packet drops and latency might be high for the considered interference scenarios, the network reliability remains at 100% for all the tests (no missed updates are observed). On the other hand, for all relevant cases (stages 2 and 3) interference management requires a larger amount of network resources (e.g., in terms of consecutive slots) that directly affects the network capacity and the number of devices supported. Finally, it should be noticed that relevant performance improvements would be observed by matching/adapting the channel hopping policy to the considered interference pattern. Interference estimation (or spectrum sensing) is therefore crucial to acquire postdeployment, detailed information about time-varying interference patterns from which ad hoc resource allocation strategies could be defined to avoid intolerable source of impairments. Interference sensing through distributed estimation processing is discussed in the following section.

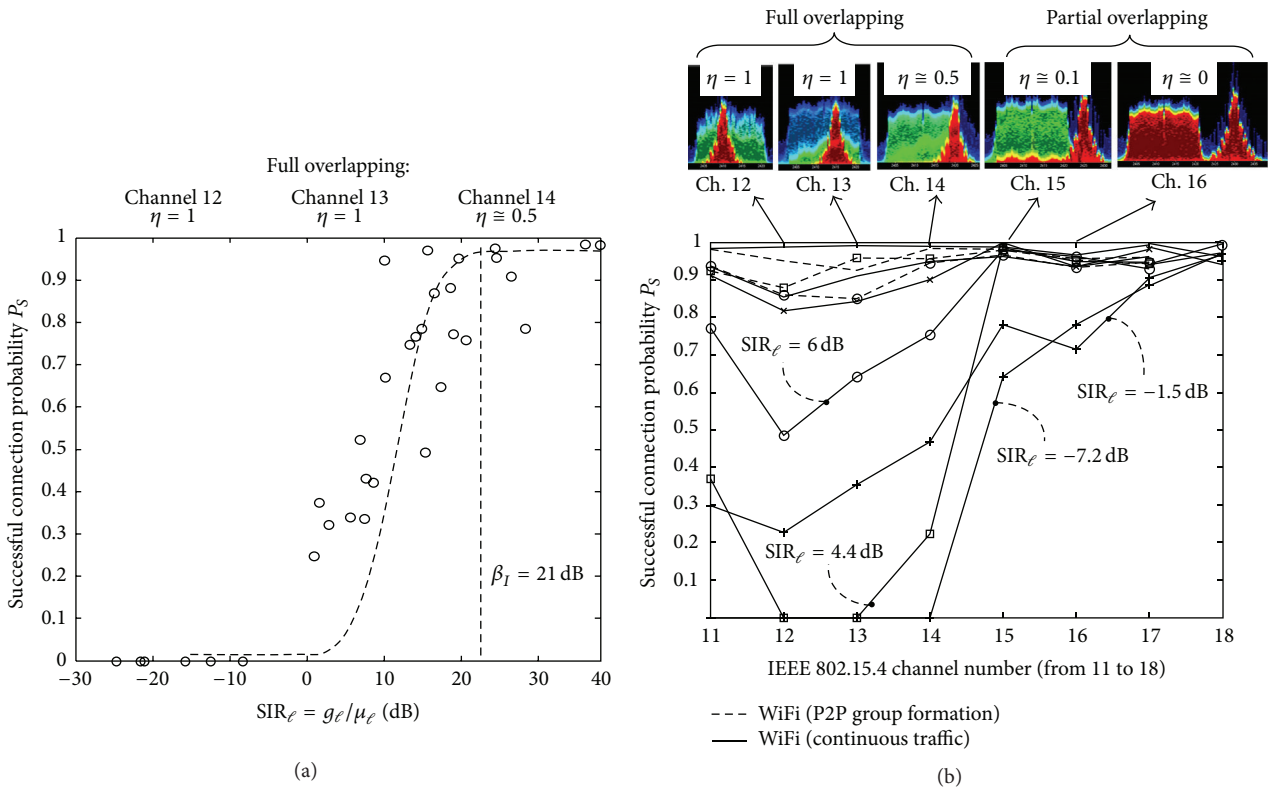


Figure 8: Coexistence results with enhanced IEEE 802.15.4 PHY data-rate devices (1 Mbit/s) with reduced spreading factor to 2. Successful probability (IEEE 802.15.4 packets) for varying SIR under full overlapping (a). Successful probability for varying WiFi-IEEE 802.15.4 overlapping (b), for selected values of SIR and traffic loads, under continuous transmission and P2P WiFi group formation. IEEE 802.15.4 PHY (enhanced PHY rate 1 Mbit/s, DSSS $Q_2 = 2$).

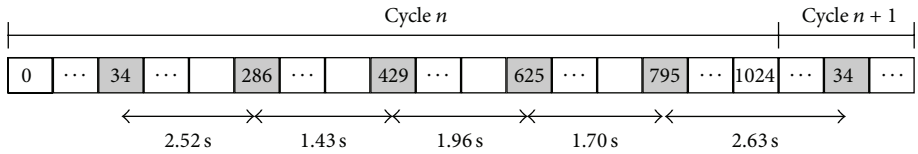


Figure 9: WH superframe and slots assigned to communication between field device and gateway.

7. Distributed Spectrum Sensing for Network Coexistence

In this section, we analyze the problem of spectrum sensing in a real scenario with two coexisting heterogeneous industrial networks sharing the same time-frequency resources. Sensing of the spectrum is a critical prerequisite in envisioned applications of wireless industrial networks: this is typically carried out during network start-up (e.g., centrally, by network manager or gateway) or during postlayout network verification [10] with the goal of identifying interfering signals that might represent intolerable sources of impairments.

In this section, we focus on a cooperative approach to spectrum sensing [20]. We consider a distributed methodology that does not require any coordination by a central unit, as it enables the local nodes (e.g., field devices) to reach a consensus on the interference pattern by simply exchanging low-overhead messages over peer-to-peer links. The experimental scenario consists of a network of field devices (here called secondary users or SUs) that are deployed to cooperatively identify the overall interference patterns caused by a preexisting network of primary devices (or primary users, PUs). Interference patterns are considered tolerable (or intolerable) based on the practical coexistence rules identified from the previous experiments (Sections 3–6): in case an intolerable interference signal is detected, the transmission resources can be scheduled over the unused portion of the spectrum [5].

Experimental tests are based on an indoor measurement campaign carried out inside the Politecnico di Milano campus. As depicted in Figure 10, the interfering signals are originated from three IEEE 802.15.4 (ZigBee compliant [21]) PU transmitters and three IEEE 802.11g (WiFi) devices acting as infrastructure access points. The ZigBee PUs are programmable devices configured to implement automatic

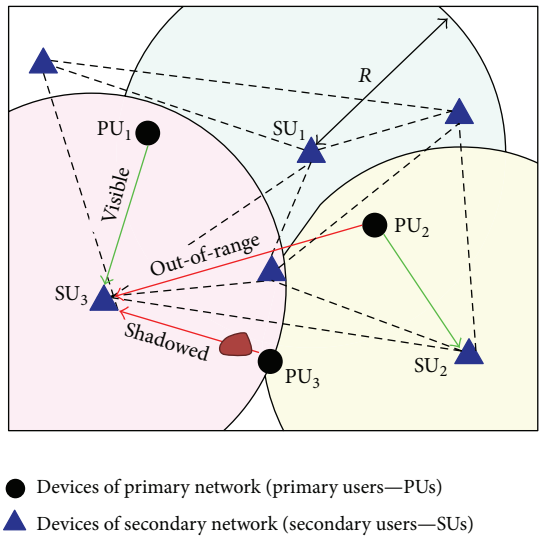


FIGURE 10: Spectrum sensing network configuration.

power and gain adjustments based on the LQI and send acknowledged data frames with application-dependent duty cycle. They perform periodic transmission over predefined (but unknown to SUs) channels with center frequencies {2.45, 2.46, 2.47} GHz (standard compliant channels {20, 22, 24}), as shown in Figure 11(a). For each channel, the occupied bandwidth is 3 MHz with nominal duty cycle of 30%. The six users of the sensing network (SUs) consist of PCs equipped with a portable spectrum analyzer operating in the 2.4 GHz band, and they might be equipped with arbitrary RF frontend (e.g., WiFi, WH, ZigBee). Power spectral measurements for interference sensing are taken with frequency steps $\Delta f \cong 333$ kHz (to cover the unlicensed 2.4÷2.495 GHz band), resolution of 187.5 kHz, and sampling time $\Delta t \cong 536$ ms (dwell time of 1 ms).

Measurements are processed to extract the RSS information from which the relevant interference patterns can be tracked. Pattern criticality can be then evaluated based on the coexistence rules highlighted in previous sections. As shown in Figure 10, due to the limited sensing range of each SU device and dynamic fading/shadowing caused by mobility, each PU transmission is overheard by a subset of the SUs in a fragmented way over time, leading to the incomplete observation of the transmission pattern, as experienced by SU_2 and SU_3 in Figure 11(a) (only three over six available SUs are shown). In this scenario with limited visibility, cooperation between SUs is crucial to detect the complete interference pattern of the primary network, thus motivating the use of a distributed policy for interference pattern reconstruction as further detailed.

A weighted-average consensus algorithm [22] is employed where SUs rely only on local processing and on repeated exchange of information with neighbors to update the interference pattern estimates. Namely, let $\boldsymbol{\theta}$ be a set of unknown parameters characterizing the PU spectrum occupancy (e.g., the interference power over time-frequency grid). The spectrum estimate at ith SU is updated at each consensus iteration q based on the local estimates provided by the neighbor devices j (in subset $\mathcal{N}_i$) as follows:

$$\widehat{\boldsymbol{\theta}}_i(q+1) = \widehat{\boldsymbol{\theta}}_i(q) + \varepsilon \mathbf{W}_i^{-1} \sum_{j \in \mathcal{N}_i} \left(\widehat{\boldsymbol{\theta}}_j(q) - \widehat{\boldsymbol{\theta}}_i(q)\right). \quad (5)$$

The weighting matrix $\mathbf{W}_i$ is designed according to [5] in order to guarantee convergence in few iterations and with reduced amount of information exchange. Consensus is nested within an iterative decision-directed (DD) procedure [23] for distributed Bayesian detection of the PU spectrum occupancy.

Figure 11(b) shows the binary masks obtained by the distributed processing procedure providing information about the time-frequency interference patterns caused by the PU primary networks. Binary masks are evaluated for both noncooperative (single-node) and distributed cooperative algorithms: each subfigure highlights the most critical interference signals from the IEEE 802.15.4 devices. In these tests, given the critical overlapping conditions identified in (3), the WiFi interfering signals can be considered noncritical disturbance; therefore, they are considered irrelevant for the interference detection goal. For all methods, we evaluate the probability of misclassification defined as the percentage of errors with respect to the centralized approach, here considered as reference. It can be seen that noncooperative detection is highly affected by errors due to partial visibility. On the other hand, the distributed method based on weighted-consensus is shown to outperform the noncooperative one reaching the same performance of the centralized detection. We can thus conclude that, throughout the cooperation between nodes, the spectrum occupancy of all critical interference sources is well reconstructed, overcoming the limits due to the reduced sensing range at single nodes and time-varying connectivity conditions (i.e., fading and shadowing effects).

8. Conclusions

This work presented an overview of coexistence issues in wireless network standards for Industrial Internet of Things. A study of PHY layer interference was proposed by introducing a model for collision probability which was validated by three different experimental setups. In order to handle dynamic and unforeseeable propagation characteristics, a first testbed was deployed in a controlled environment to evaluate the IEEE 802.15.4 sensitivity against IEEE 802.11 interference. Results highlighted tolerable power thresholds for IEEE 802.15.4 devices to coexist with IEEE 802.11 equipment for different levels of interference overlapping. Channels with full overlapping presented a minimum SIR equal to 15 dB and cochannel interference with a SIR not higher than −21,9 dB. A second setup of experiments was carried out in an open (mixed LOS/NLOS) environment to evaluate also the impact of different IEEE 802.15.4 data-rate selections. Results showed values of threshold SIR in the order of 15 dB and 21 dB for 250 kbps and 1 Mbit/s, respectively, for 99% successful connection probability in the worst-case scenario (considering high-data rate and full overlapping channel).

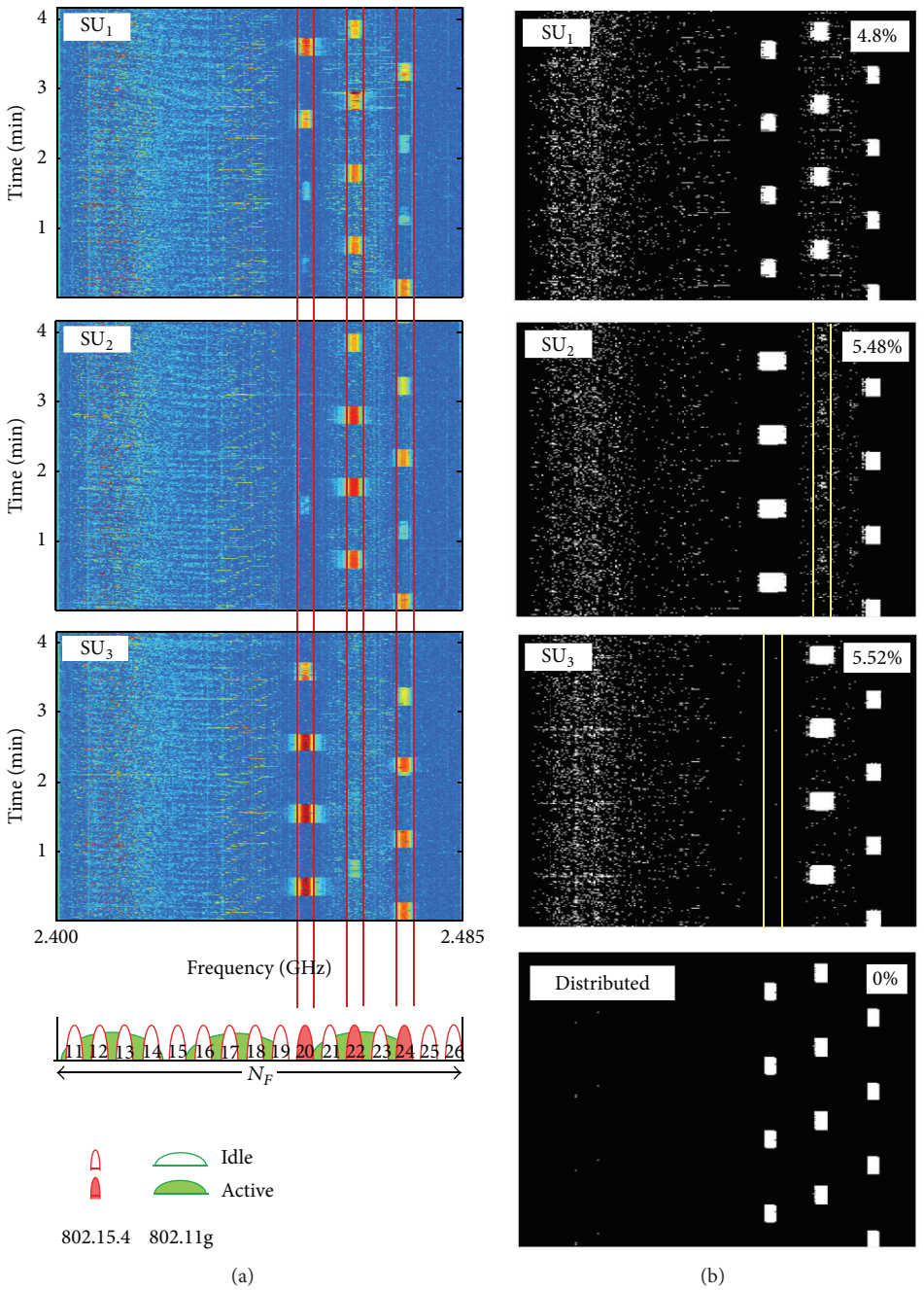


Figure 11: (a) Spectrum sensing by three IEEE 802.15.4 SUs collecting RSS measurements over time and frequency. PUs perform periodic transmission tasks over the IEEE 802.15.4 channels 20, 22, and 24. Three WiFi devices are also interfering in the same 2.4 GHz band. (b) Time-frequency spectrum detection by noncooperative processing at node SU_i, $i = 1, \ldots, 3$ (on top), and by the cooperative distributed approach (on bottom). Yellow boxes highlight the misclassification due to the effects of partial visibility for SU_2 and SU_3. The probability of misclassification is shown in the top-right corner of each subfigure.

Despite the radio propagation effects observed in this experiment (multipath, fading signal, blockages, etc.), this result is very similar to the one obtained in the confined environment. Another experiment evaluation was related to *Wireless*HART full stack performance under interference conditions. A test setup was proposed to measure the reliability and the network latency for three relevant scenarios.

Practical rules were discussed to support device deployment and postlayout interference testing in a specific area. Spectrum sensing of multiple interfering signals was implemented by a cooperative network of sensing devices by distributed consensus-based processing. Interference patterns were considered tolerable (or intolerable) based on the coexistence rules identified in the first part of the work, in order to enable scheduling of the transmission resources (e.g., the channel hopping policy) over the allowed portions of the spectrum. The analysis aimed to provide a better understanding of protocol limitations, as support for the

design of advanced interference management policies (as envisioned for future industry-level standards).

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work has been partially performed in the framework of the EU research project DIWINE (Dense Cooperative Wireless Cloud Network) under FP7 ICT Objective 1.1—The Network of the Future. The authors would like to express their gratitude to CNPq and Capes on their support for this work. They also thank Petrobras and Finep.

References

[1] N. P. Mahalik, Ed., *Fieldbus Technology: Industrial Network Standards for Real-Time Distributed Control*, Springer Science & Business Media, 2003.

[2] M. Abdul Ghayum, *Comparative study of wireless protocols: wi-Fi, bluetooth, zigBee, wirelessHART and ISA SP100, and their effectiveness in industrial automation [M.S. thesis]*, University of Texas at Austin, 2011.

[3] B. O'hara and A. Petrick, *IEEE 802.11 Handbook: A Designer's Companion*, Wiley, IEEE Standards Association, 2005.

[4] W. Guo, W. M. Healy, and M. Zhou, "Impacts of 2.4-GHz ISM band interference on IEEE 802.15.4 wireless sensor network reliability in buildings," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 9, pp. 2533–2544, 2012.

[5] G. Soatti, M. Nicoli, S. Savazzi, and U. Spagnolini, "Distributed sensing of interference pattern in dense cooperative wireless networks," in *Proceedings of the IEEE International Conference on Communication Workshop (ICCW '15)*, pp. 961–966, IEEE, London, UK, June 2015.

[6] IEEE Std. 802.15.4-2006, *Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Computer Society, New York, NY, USA, 2006.

[7] L. Doherty and D. A. Teasdale, "Towards 100% reliability in wireless monitoring networks," in *Proceedings of the 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, pp. 132–135, ACM, Malaga, Spain, October 2006.

[8] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: the format war hits the factory floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, 2011.

[9] N. Baccour, A. Koubaa, L. Mottola et al., "Radio link quality estimation in wireless sensor networks: a survey," *ACM Transactions on Sensor Networks*, vol. 8, no. 4, article 34, 2012.

[10] R. H. de Souza, S. Savazzi, and L. B. Becker, "Network design and planning of wireless embedded systems for industrial automation," *Design Automation for Embedded Systems*, vol. 19, no. 4, pp. 367–388, 2015.

[11] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, "Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 8, pp. 1514–1523, 2008.

[12] Freescale, "MKW2xDxxx Data Sheet," kw20x datasheet, November 2013.

[13] S. Savazzi, V. Rampa, and U. Spagnolini, "Wireless Cloud Networks for the Factory of Things: connectivity modeling and layout design," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 180–195, 2014.

[14] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, and P. Demeester, "Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment," *Eurasip Journal on Wireless Communications and Networking*, vol. 2012, article 137, 2012.

[15] D. Yang, Y. Xu, and M. Gidlund, "Wireless coexistence between IEEE 802.11- and IEEE 802.15.4-based networks: a survey," *International Journal of Distributed Sensor Networks*, vol. 2011, Article ID 912152, 17 pages, 2011.

[16] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with WiFi direct: overview and experimentation," *IEEE Wireless Communications*, vol. 20, no. 3, pp. 96–104, 2013.

[17] Z. Iqbal, M. Gidlund, and J. Åkerberg, "Deterministic and event triggered MAC protocol for industrial wireless networks," in *Proceedings of the IEEE International Conference on Industrial Technology (ICIT '13)*, pp. 1252–1259, Cape Town, South Africa, February 2013.

[18] J. Song, S. Han, A. K. Mok et al., "WirelessHART: applying wireless technology in real-time industrial process control," in *Proceedings of the 14th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS '08)*, pp. 377–386, IEEE, St. Louis, Mo, USA, April 2008.

[19] J. M. Winter, C. Lima, I. Muller, C. E. Pereira, and J. C. Netto, "WirelessHART routing analysis software," in *Proceedings of the 1st Brazilian Symposium on Computing System Engineering (SBESC '11)*, pp. 96–98, Florianópolis, Brazil, November 2011.

[20] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, pp. 1658–1663, IEEE, Istanbul, Turkey, July 2006.

[21] NXP Laboratories, *Data-Sheet JN-DS-JN5148-001, IEEE 802.15.4 Wireless Microcontroller JN5148-001*, NXP Laboratories, Sheffield, UK, 2012.

[22] M. Nicoli, G. Soatti, and S. Savazzi, "Distributed estimation of macroscopic channel parameters in dense cooperative wireless networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14)*, pp. 972–977, Istanbul, Turkey, April 2014.

[23] U. Spagnolini, "Cancellation of polarized impulsive noise using an azimuth-dependent conditional mean estimator," *IEEE Transactions on Signal Processing*, vol. 46, no. 12, pp. 3333–3344, 1998.